UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,794	12/30/2003	Emily H. Qi	10559-898001 / P17946	5375

20985 7590 08/31/2007

FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
LOUIE, OSCAR A	
ART UNIT	**PAPER NUMBER**
2136	

MAIL DATE	DELIVERY MODE
08/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

mN

Office Action Summary	Application No.	Applicant(s)	
	10/749,794	QI ET AL.	
	Examiner	Art Unit	
	Oscar A. Louie	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 October 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *06/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This first non-final action is in response to the original filing of 12/30/2003. Claims 1-47 are pending and has/have been considered as follows.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 37-39 & 42-44 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- Regarding claims 37-39 & 42-44, the term "capable" renders the claims indefinite because it is unclear whether the limitation(s) following the term are capable/incapable of being performing or are a part of the claimed invention.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-3, 5, 13, 20, 21, 23-26, 29, 31, 33, 35-37, 40-43 rejected under 35 U.S.C. 102(e) as being anticipated by Ekberg (US-7003282-B1).

Claim 1:

Ekberg discloses a machine-implemented method comprising,

- "producing a first authentication message" (i.e. "The terminal (the Kerberos client) sends to the ticket-granting server such a request in accordance with the Kerberos protocol, which contains the name (s, e.g. terminal B) of that server, for which the ticket is desired") [column 9 lines 60-63];
- "authentication data encrypted with a first key" (i.e. "a ticket T.sub.c,tgs encrypted with the ticket granting server's own key K.sub.tgs for access to the ticket-granting service and an authenticator Ac, which is encrypted with a connection-specific key K.sub.c,tgs") [column 9 lines 64-66];
- "a data structure comprising the first key" (i.e. "Thereupon the Kerberos server generates a ticket Tc,tgs, with which the client may use the ticket-granting service") [column 8 lines 46-48];
- "wherein the data structure is encrypted with a second key" (i.e. "This ticket is encrypted using key K.sub.tgs") [column 8 line 54];

- "generating a request message to have a first network device associated with a first network deliver datagrams destined for a home address associated with a mobile device on the first network to a second address on a second, different network" (i.e. "The last-mentioned performs checks with the mobile node's home agent, registers the mobile node and sends the registration information to it. Packets addressed to the mobile node are sent to the mobile node's original location (to the home agent), thence they are relayed further to the current foreign agent, which will forward them to the mobile node") [column 3 lines 53-59];
- "embedding the authentication message in the request message" (i.e. "Then the Kerberos server transmits as a response to the client a packet, which contains the encrypted ticket and a copy of the connection-specific key K.sub.c,tgs") [column 8 lines 56-58].

Claim 2:

Ekberg discloses a machine-implemented method, as in Claim 1 above, further comprising,

- "the authentication data comprises a timestamp" (i.e. "timestamp") [column 10 line 3].

Claim 3:

Ekberg discloses a machine-implemented method, as in Claim 1 above, further comprising,

- "the second key is known to the first network device and unknown to the mobile node" (i.e. "This ticket is encrypted using key K.sub.tgs, which is known only to the ticket-granting server and to the Kerberos server") [column 8 lines 54-56].

Claim 5:

Ekberg discloses a machine-implemented method, as in Claim 1 above, further comprising,

- "the data structure comprises a Kerberos ticket" (i.e. "the Kerberos server generates a ticket") [column 8 lines 46-47].

Claim 13:

Ekberg discloses a machine-implemented method, as in Claim 1 above, further comprising,

- "the request message comprises a Registration Request message" (i.e. "the terminal sends a RR (Registration Request)") [column 5 lines 3-4].

Claim 20:

Ekberg discloses a machine-implemented method comprising,

- "receiving at a first device associated with a home network an authentication message and a request message to reroute datagrams destined for a first address of a mobile device associated with the home network to a second address not associated with the home network" (i.e. "The last-mentioned performs checks with the mobile node's home agent, registers the mobile node and sends the registration information to it. Packets addressed to the mobile node are sent to the mobile node's original location (to the home agent), thence they are relayed further to the current foreign agent, which will forward them to the mobile node") [column 3 lines 53-59];
- "wherein the request message comprises: a data structure that includes a first key encrypted with a second key" (i.e. "Thereupon the Kerberos server generates a ticket Tc,tgs, with which the client may use the ticket-granting service... This ticket is encrypted using key K.sub.tgs") [column 8 lines 46-48 & 54];

- "determining if the authentication message is valid" (i.e. "The ticket-granting server checks the authenticator's information and the ticket T.sub.c,tgs") [column 10 lines 4-5].

Claim 21:

Ekberg discloses a machine-implemented method, as in Claim 20 above, further comprising,

- "generating a third key if the authentication message is determined to be valid" (i.e. "If the ticket is all right, the ticket-granting server generates a new random session key K.sub.c,s") [column 10 lines 5-8].

Claim 23:

Ekberg discloses a machine-implemented method, as in Claim 20 above, further comprising,

- "the authentication message comprises a hash of the request message" (i.e. "The registration is based on a check value calculated from the registration message (from the registration request or reply)") [column 5 lines 25-29];
- "wherein the hash is computed using the first key" (i.e. "The registration is based on a check value calculated from the registration message (from the registration request or reply), and the registration must be made only between that mobile node and that home agent, which have a shared fixed key (which is agreed upon in advance)") [column 5 lines 25-29].

Claim 24:

Ekberg discloses a machine-implemented method, as in Claim 20 above, further comprising,

- "the request message comprises a Registration Request message" (i.e. "the terminal sends a RR (Registration Request)") [column 5 lines 3-4].

Claim 25:

Ekberg discloses a machine-implemented method, as in Claim 23 above, further comprising,

- "determining if the authentication message is valid comprises: computing a hash of the request message using the first key" (i.e. "The registration is based on a check value calculated from the registration message (from the registration request or reply), and the registration must be made only between that mobile node and that home agent, which have a shared fixed key (which is agreed upon in advance)") [column 5 lines 25-29];
- "determining if the authentication message is valid comprises: comparing the computed hash to the authentication message" (i.e. "The registration is based on a check value calculated from the registration message (from the registration request or reply), and the registration must be made only between that mobile node and that home agent, which have a shared fixed key (which is agreed upon in advance)") [column 5 lines 25-29].

Claim 26:

Ekberg discloses a machine-implemented method, as in Claim 25 above, further comprising,

- "decrypting the data structure using the second key to obtain the first key" (i.e. "The terminal of the third party gets the recently generated session key K.sub.c,s from the ticket by first decrypting the ticket with its own key Kc") [column 10 lines 17-19].

Claim 29:

Ekberg discloses a computer program product residing on a computer readable medium having instructions stored thereon comprising,

- "form an authentication message" (i.e. "The terminal (the Kerberos client) sends to the ticket-granting server such a request in accordance with the Kerberos protocol, which contains the name (s, e.g. terminal B) of that server, for which the ticket is desired") [column 9 lines 60-63];
- "authentication data encrypted with a first key" (i.e. "a ticket T.sub.c,tgs encrypted with the ticket granting server's own key K.sub.tgs for access to the ticket-granting service and an authenticator Ac, which is encrypted with a connection-specific key K.sub.c,tgs") [column 9 lines 64-66];
- "the first key encrypted with a second key" (i.e. "This ticket is encrypted using key K.sub.tgs") [column 8 line 54];
- "generate a request message requesting that datagrams destined for a first Internet Protocol address of a mobile device be routed to a second Internet Protocol address" (i.e. "The last-mentioned performs checks with the mobile node's home agent, registers the mobile node and sends the registration information to it. Packets addressed to the mobile node are sent to the mobile node's original location (to the home agent), thence they are relayed further to the current foreign agent, which will forward them to the mobile node") [column 3 lines 53-59];

- "include the authentication request message in the request message" (i.e. "Then the Kerberos server transmits as a response to the client a packet, which contains the encrypted ticket and a copy of the connection-specific key K.sub.c,tgs") [column 8 lines 56-58].

Claim 31:

Ekberg discloses a computer program product residing on a computer readable medium having instructions stored thereon, as in Claim 29 above, further comprising,

- "instructions to generate a hash of the request message using the first key to form a second authentication message" (i.e. "The registration is based on a check value calculated from the registration message (from the registration request or reply)") [column 5 lines 25-29].

Claim 33:

Ekberg discloses a computer program product residing on a computer readable medium having instructions stored thereon comprising,

- "extract an authentication message from a message requesting that datagrams destined for a first Internet Protocol address of a mobile device be routed to a second Internet Protocol address" (i.e. "The terminal (the Kerberos client) sends to the ticket-granting server such a request in accordance with the Kerberos protocol, which contains the name (s, e.g. terminal B) of that server, for which the ticket is desired") [column 9 lines 60-63];

- "wherein the authentication message comprises: authentication data encrypted with a first key" (i.e. "a ticket T.sub.c,tgs encrypted with the ticket granting server's own key K.sub.tgs for access to the ticket-granting service and an authenticator Ac, which is encrypted with a connection-specific key K.sub.c,tgs") [column 9 lines 64-66];
- "wherein the authentication message comprises: a data structure comprising the first key, and encrypted with a second key" (i.e. "Thereupon the Kerberos server generates a ticket Tc,tgs, with which the client may use the ticket-granting service... This ticket is encrypted using key K.sub.tgs") [column 8 lines 46-48 & 54];
- "verify the authentication data" (i.e. "If the ticket is all right, the ticket-granting server generates a new random session key K.sub.c,s") [column 10 lines 5-8];
- "if the authentication data is valid, then generating a third key" (i.e. "If the ticket is all right, the ticket-granting server generates a new random session key K.sub.c,s") [column 10 lines 5-8].

Claim 35:

Ekberg discloses a computer program product residing on a computer readable medium having instructions stored thereon, as in Claim 33 above, further comprising,

- "instructions that cause the processor to: store the encryption key" [Fig 8 illustrates storage].

Claim 36:

Ekberg discloses a computer program product residing on a computer readable medium having instructions stored thereon, as in Claim 33 above, further comprising,

- "the message comprises a Registration Request message" (i.e. "the terminal sends a RR (Registration Request)") [column 5 lines 3-4].

Claim 37:

Ekberg discloses a system comprising,

- "a first network device associated with a first network" (i.e. "the router will notice that the user has entered the network") [column 11 lines 55-58];
- "a second network device associated with the first network" (i.e. "the network must include a separate "locating agent", which by monitoring or "pinging" the router") [column 10 lines 22-23];
- "the second network device capable of: producing an authentication message including a data structure comprising the first key with the data structure encrypted with a second key" (i.e. "Thereupon the Kerberos server generates a ticket Tc,tgs, with which the client may use the ticket-granting service... This ticket is encrypted using key K.sub.tgs...The terminal (the Kerberos client) sends to the ticket-granting server such a request in accordance with the Kerberos protocol, which contains the name (s, e.g. terminal B) of that server, for which the ticket is desired") [column 8 lines 46-48 & 54 and column 9 lines 60-63];

- "generating a request message to have the first network device deliver datagrams destined for a home address associated with the second device on the first network to a second address on a second, different network" (i.e. "The last-mentioned performs checks with the mobile node's home agent, registers the mobile node and sends the registration information to it. Packets addressed to the mobile node are sent to the mobile node's original location (to the home agent), thence they are relayed further to the current foreign agent, which will forward them to the mobile node") [column 3 lines 53-59];
- "including the authentication message within the request message" (i.e. "Then the Kerberos server transmits as a response to the client a packet, which contains the encrypted ticket and a copy of the connection-specific key K.sub.c,tgs") [column 8 lines 56-58].

Claim 40:

Ekberg discloses a system, as in Claim 37 above, further comprising,

- "the first network device is a router" (i.e. "by monitoring or "pinging" the router will notice that the user has entered the network") [column 11 lines 55-58].

Claim 41:

Ekberg discloses a system, as in Claim 37 above, further comprising,

- "the second network device is a laptop computer" (i.e. "a portable computer (with software)") [column 4 lines 31-32].

Claim 42:

Ekberg discloses a system, as in Claim 37 above, further comprising,

- "a third device capable of producing the first key and the data structure encrypted with the second key" (i.e. "Thereupon the Kerberos server generates a ticket Tc,tgs, with which the client may use the ticket-granting service... This ticket is encrypted using key K.sub.tgs") [column 8 lines 46-48 & 54].

Claim 43:

Ekberg discloses a system comprising,

- "a router associated with a first network" (i.e. "the router will notice that the user has entered the network") [column 11 lines 55-58];
- "an input port for receiving datagrams" (i.e. "the network must include a separate "locating agent", which by monitoring or "pinging" the router") [column 11 lines 54-55];
- "a switch fabric for determining destination of datagrams" (i.e. "The last-mentioned performs checks with the mobile node's home agent, registers the mobile node and sends the registration information to it. Packets addressed to the mobile node are sent to the mobile node's original location (to the home agent), thence they are relayed further to the current foreign agent, which will forward them to the mobile node") [column 3 lines 53-59];
- "a processor capable of: reading request message to reroute datagrams destined for a first address of a mobile device associated with the first network to a second address associated with a second, different network" (i.e. "The last-mentioned performs checks with the mobile node's home agent, registers the mobile node and sends the registration

information to it. Packets addressed to the mobile node are sent to the mobile node's original location (to the home agent), thence they are relayed further to the current foreign agent, which will forward them to the mobile node") [column 3 lines 53-59];

- "wherein the request message includes a data structure comprising a first key unknown to the processor encrypted with a second key that is known to the processor" (i.e. "Thereupon the Kerberos server generates a ticket Tc,tgs, with which the client may use the ticket-granting service... This ticket is encrypted using key K.sub.tgs") [column 8 lines 46-48 & 54];
- "verifying an authentication message associated with the request message" (i.e. "If the ticket is all right, the ticket-granting server generates a new random session key K.sub.c,s") [column 10 lines 5-8];
- "wherein the authentication message comprises a hashed version of the request message computed using the first key" (i.e. "The registration is based on a check value calculated from the registration message (from the registration request or reply)") [column 5 lines 25-29];
- "if the authentication message is valid, then generating a third key" (i.e. "If the ticket is all right, the ticket-granting server generates a new random session key K.sub.c,s") [column 10 lines 5-8].

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 4, 6-12, 14-19, 22, 27, 28, 30, 32, 34, 38, 39, & 44-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ekberg (US-7003282-B1).

Claim 4:

Ekberg discloses a machine-implemented method, as in Claim 1 above, but does not explicitly disclose,

- "the authentication message comprises a Kerberos Application Request"

however, Ekberg does disclose,

- "the terminal sends a RR (Registration Request) to its own home agent through foreign agent" [column 5 line 9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the authentication message comprises a Kerberos Application Request," in the invention as disclosed by Ekberg since any request sent by the client/terminal (i.e. mobile device) that involves a Kerberos server would imply that there would be Kerberos requests for various services (i.e. Applications).

Claim 6:

Ekberg discloses a machine-implemented method, as in Claim 1 above, but does not explicitly disclose,

- "generating a second authentication message"

however, Ekberg does disclose,

- "The terminal (the Kerberos client) sends to the ticket-granting server such a request in accordance with the Kerberos protocol" [column 9 lines 60-63];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "generating a second authentication message," in the invention as disclosed by Ekberg since a Kerberos server/system would be used by many terminals and devices which implies the creation/generation of many requests and messages (i.e. first/second/third/etc authentication messages).

Claim 7:

Ekberg discloses a machine-implemented method, as in Claim 6 above, further comprising,

- "generating a hash of the request message using the first key" (i.e. "The registration is based on a check value calculated from the registration message (from the registration request or reply), and the registration must be made only between that mobile node and that home agent, which have a shared fixed key (which is agreed upon in advance)") [column 5 lines 25-29].

Claim 8:

Ekberg discloses a machine-implemented method, as in Claim 6 above, further comprising,

- "transmitting the request message and second authentication message to the first network device" (i.e. "The last-mentioned performs checks with the mobile node's home agent, registers the mobile node and sends the registration information to it. Packets addressed to the mobile node are sent to the mobile node's original location (to the home agent), thence they are relayed further to the current foreign agent, which will forward them to the mobile node") [column 5 lines 25-29].

Claim 9:

Ekberg discloses a machine-implemented method, as in Claim 8 above, further comprising,

- "receiving the request message and second authentication message by a device on the home network" (i.e. "The last-mentioned performs checks with the mobile node's home agent, registers the mobile node and sends the registration information to it. Packets addressed to the mobile node are sent to the mobile node's original location (to the home agent), thence they are relayed further to the current foreign agent, which will forward them to the mobile node") [column 3 lines 53-59];
- "decrypting the data structure using the second key to obtain the first key" (i.e. "The terminal of the third party gets the recently generated session key K.sub.c,s from the ticket by first decrypting the ticket with its own key Kc") [column 10 lines 17-19].

Claim 10:

Ekberg discloses a machine-implemented method, as in Claim 9 above, further comprising,

- "verifying the second authentication message using the first key" (i.e. "Thereafter the new session key is available to both terminals and encrypted data transmission may begin") [column 10 lines 19-21].

Claim 11:

Ekberg discloses a machine-implemented method, as in Claim 9 above, further comprising,

- "generating a third key" (i.e. "If it does, it will generate a random connection-specific key K.sub.c,tgs, which will be used later in data transmission between the client and the ticket-granting server") [column 8 lines 43-44].

Claim 12:

Ekberg discloses a machine-implemented method, as in Claim 9 above, further comprising,

- "generating key material" (i.e. "If it does, it will generate a random connection-specific key K.sub.c,tgs, which will be used later in data transmission between the client and the ticket-granting server") [column 8 lines 43-44];
- "wherein the key material-may be supplied to a function to generate a third key" (i.e. "it will generate a random connection-specific key K.sub.c,tgs") [column 8 lines 43-44].

Claim 14:

Ekberg discloses a machine-implemented method, as in Claim 11 above, further comprising,

- "forming a reply authentication message comprising the third key encrypted with the first key" (i.e. "Then the ticket-granting server forms a new ticket T.sub.c,s for the said third party, encrypts the ticket using the said third party's own key K.sub.s, which is the same as the concerned subscriber's key Kc described above, and transmits the encrypted key together with the session key to the terminal") [column 10 lines 9-13].

Claim 15:

Ekberg discloses a machine-implemented method, as in Claim 14 above, but does not explicitly disclose,

- "the reply authentication message comprises a Kerberos Application Reply message"

however, Ekberg does disclose,

- "the terminal sends a RR (Registration Request) to its own home agent through foreign agent" [column 5 line 9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the reply authentication message comprises a Kerberos Application Reply message," in the invention as disclosed by Ekberg since any request sent by the client/terminal (i.e. mobile device) that involves a Kerberos server would imply that there would be Kerberos requests for various services (i.e. Applications).

Claim 16:

Ekberg discloses a machine-implemented method, as in Claim 14 above, further comprising,

- "forming a reply message that includes the reply authentication message" (i.e. "In the reply message there is all the necessary information indicating how (on what conditions) the home agent has accepted the registration request") [column 5 lines 10-12].

Claim 17:

Ekberg discloses a machine-implemented method, as in Claim 16 above, further comprising,

- "the reply message comprises a Registration Reply message" (i.e. "the terminal sends a RR (Registration Request) to its own home agent through foreign agent") [column 5 line 9].

Claim 18:

Ekberg discloses a machine-implemented method, as in Claim 14 above, further comprising,

- "transmitting the reply message and third authentication message to the mobile node" (i.e. "The last-mentioned performs checks with the mobile node's home agent, registers the mobile node and sends the registration information to it. Packets addressed to the mobile node are sent to the mobile node's original location (to the home agent), thence they are relayed further to the current foreign agent, which will forward them to the mobile node") [column 3 lines 53-59];

but does not explicitly disclose,

- "generating a third authentication message"

however, Ekberg does disclose,

- "The terminal (the Kerberos client) sends to the ticket-granting server such a request in accordance with the Kerberos protocol" [column 9 lines 60-63];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "generating a third authentication message," in the invention as disclosed by Ekberg since a Kerberos server/system would be used by many terminals and devices which implies the creation/generation of many requests and messages (i.e. first/second/third/etc authentication messages).

Claim 19:

Ekberg discloses a machine-implemented method, as in Claim 18 above, further comprising,

- "generating a hash of the reply authentication message using the first key" (i.e. "The registration is based on a check value calculated from the registration message (from the registration request or reply), and the registration must be made only between that mobile node and that home agent, which have a shared fixed key (which is agreed upon in advance)") [column 5 lines 25-29].

Claim 22:

Ekberg discloses a machine-implemented method, as in Claim 20 above, further comprising,

- "generating key material if the authentication message is determined to be valid" (i.e. "If the ticket is all right, the ticket-granting server generates a new random session key K.sub.c,s") [column 10 lines 5-8];

but does not explicitly disclose,

- "wherein the key material may be supplied to a function known to the first device and the mobile device to produce a third key"

however, Ekberg does disclose,

- "it will generate a random connection-specific key K.sub.c,tgs" [column 8 lines 43-44];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the key material may be supplied to a function known to the first device and the mobile device to produce a third key," in the invention as disclosed by Ekberg since the key is generated based on random connection-specific information and it is implied that a different key would be generated each time (i.e. first/second/third/etc keys).

Claim 27:

Ekberg discloses a machine-implemented method, as in Claim 21 above, further comprising,

- "receiving a reply message from the first device by the mobile device" [Fig 7 illustrates requests and reply messages];

but does not explicitly disclose,

- "wherein the reply message includes the third key"

however, Ekberg does disclose,

- [Fig 7 illustrates a key which would be one of many keys];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the reply message includes the third key," in the invention as disclosed by Ekberg since it is understood that for each request from each device, a different key would be generated (i.e. first/second/third/etc keys).

Claim 28:

Ekberg discloses a machine-implemented method, as in Claim 27 above, further comprising,

- "transmitting the second request message and second authentication message to the first device" (i.e. "The last-mentioned performs checks with the mobile node's home agent, registers the mobile node and sends the registration information to it. Packets addressed to the mobile node are sent to the mobile node's original location (to the home agent), thence they are relayed further to the current foreign agent, which will forward them to the mobile node") [column 3 lines 53-59];

but does not explicitly disclose,

- "forming a second request message to have datagrams destined for a first address of a mobile device associated with the home network to a third address not associated with the home network"
- "forming a second authentication message using the third key"

however, Ekberg does disclose,

- "The last-mentioned performs checks with the mobile node's home agent, registers the mobile node and sends the registration information to it. Packets addressed to the mobile node are sent to the mobile node's original location (to the home agent), thence they are relayed further to the current foreign agent, which will forward them to the mobile node" [column 3 lines 53-59];
- "The terminal (the Kerberos client) sends to the ticket-granting server such a request in accordance with the Kerberos protocol" [column 9 lines 60-63];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "forming a second request message to have datagrams destined for a first address of a mobile device associated with the home network to a third address not associated with the home network" and "forming a second authentication message using the third key," in the invention as disclosed by Ekberg since it is understood from Ekberg's disclosure that each device would communicate with the Kerberos server/system and the relaying of information among the mobile device, home agent, and foreign agent implies that several authentication messages would be exchanged between each of these nodes and the Kerberos server. Thus, also implying that several keys would be generated (i.e. first/second/third/etc keys).

Claim 30:

Ekberg discloses a computer program product residing on a computer readable medium having instructions stored thereon, as in Claim 29 above, but does not explicitly disclose,

- "the authentication message comprises a Kerberos Application Request message"

however, Ekberg does disclose,

- "the terminal sends a RR (Registration Request) to its own home agent through foreign agent" [column 5 line 9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the authentication message comprises a Kerberos Application Request message," in the invention as disclosed by Ekberg since any request sent by the client/terminal (i.e. mobile device) that involves a Kerberos server would imply that there would be Kerberos requests for various services (i.e. Applications).

Claim 32:

Ekberg discloses a computer program product residing on a computer readable medium having instructions stored thereon, as in Claim 29 above, further comprising,

- "receive a reply message from the first device by the mobile device" [Fig 7 illustrates request and reply messages];

but does not explicitly disclose,

- "wherein the reply message includes a third key"
- "form a second authentication message using the third key"
- "transmit a second request message to have datagrams destined for a first address of a mobile device associated with the home network to a third address not associated with the home network"
- "wherein the second authentication message is included in the second request message"

however, Ekberg does disclose,

- [Fig 7 illustrates a key which would be one of many];
- "The terminal (the Kerberos client) sends to the ticket-granting server such a request in accordance with the Kerberos protocol" [column 9 lines 60-63];
- "The last-mentioned performs checks with the mobile node's home agent, registers the mobile node and sends the registration information to it. Packets addressed to the mobile node are sent to the mobile node's original location (to the home agent), thence they are relayed further to the current foreign agent, which will forward them to the mobile node" [column 3 lines 53-59];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the reply message includes a third key" and "form a second authentication message using the third key" and "transmit a second request message to have datagrams destined for a first address of a mobile device associated with the home network to a third address not associated with the home network" and "wherein the second authentication message is included in the second request message," in the invention as disclosed by Ekberg since it is understood from Ekberg's disclosure that each device would communicate with the Kerberos server/system and the relaying of information among the mobile device, home agent, and foreign agent implies that several authentication messages would be exchanged between each of these nodes and the Kerberos server. Thus, also implying that several keys would be generated (i.e. first/second/third/etc keys).

Claim 34:

Ekberg discloses a computer program product residing on a computer readable medium having instructions stored thereon, as in Claim 33 above, further comprising,

- "transmit the reply message to a device associated with the request message" [Fig 7 illustrates request and reply messages];

but does not disclose,

- "form a reply message that includes the third key"

however, Ekberg does disclose,

- [Fig 7 illustrates a key which would be one of many];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "form a reply message that includes the third key," in the invention as disclosed by Ekberg since it is understood that for each request from each device, a different key would be generated (i.e. first/second/third/etc keys).

Claim 38:

Ekberg discloses a system, as in Claim 37 above, but does not explicitly disclose,

- "the second network device is further capable of forming a second authentication message by computing a hash of the request message using the first key"

however, Ekberg does disclose,

- "The registration is based on a check value calculated from the registration message (from the registration request or reply)... The terminal (the Kerberos client) sends to the ticket-granting server such a request in accordance with the Kerberos protocol, which contains the name (s, e.g. terminal B) of that server, for which the ticket is desired" [column 5 lines 25-29 and column 9 lines 60-63];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the second network device is further capable of forming a second authentication message by computing a hash of the request message using the first key," in the invention as disclosed by Ekberg since a check value is a hash and it is implied that with the use of a Kerberos server/system, there would be many authentication messages (i.e. first/second/third/etc messages).

Claim 39:

Ekberg discloses a system, as in Claim 38 above, further comprising,

- "the first network device is capable of receiving the request message and generating a key if the second authentication message is valid" (i.e. "If the ticket is all right, the ticket-granting server generates a new random session key K.sub.c,s") [column 10 lines 5-8].

Claim 44:

Ekberg discloses a system, as in Claim 43 above, but does not explicitly disclose,

- "the processor is further capable of: encrypting the third key"

however, Ekberg does disclose,

- "the ticket-granting server generates a new random session key K.sub.c,s... encrypts the ticket using the said third party's own key K.sub.s" [column 10 lines 6-13];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the processor is further capable of: encrypting the third key," in the invention as disclosed by Ekberg since the encryption of a key/ticket containing a key is disclosed by Ekberg and is performed by different devices. Thus, it is implied that these devices (i.e. mobile device/home agent/foreign agent/Kerberos server/etc) would have processors/microprocessors for performing tasks (e.g. encryption).

Claim 45:

Ekberg discloses a system, as in Claim 44 above, but does not explicitly disclose,

- "the processor is further capable of: forming a reply message"
- "wherein the reply message includes the encrypted third key"
- "forming a reply authentication message"

however, Ekberg does disclose,

- [Fig 7 illustrates reply messages and a key which would be one of many];
- [Fig 2 illustrates request and reply messages];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the processor is further capable of: forming a reply message" and "wherein the reply message includes the encrypted third key" and "forming a reply authentication message," in the invention as disclosed by Ekberg since it is understood by Ekberg's disclosure that there would be numerous requests and replies among the devices which would imply that there are many keys included (i.e. first/second/third/etc keys).

Claim 46:

Ekberg discloses a system, as in Claim 45 above, further comprising,

- "the reply authentication message comprises a hashed version of the reply message" (i.e. "The registration is based on a check value calculated from the registration message (from the registration request or reply)") [column 5 lines 25-29].

Claim 47:

Ekberg discloses a system, as in Claim 45 above, further comprising,

- "transmitting the reply message and the reply authentication message to the mobile device at the second address" [Fig 2 illustrates several request and reply messages among the terminal (i.e. mobile device), home agent, foreign agent, security server (i.e. Kerberos), etc].

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
08/29/2007

Nasser Moazzami
Supervisory Patent Examiner